Revista de Divulgação Científica em
Ciências Exatas e Tecnológicas
PORANDU
Vol. 3, n. 1, 2019, pg. 1-8

Fundamentos de design combinatórios e aplicações em códigos

J. R. O. MOREIRA [1,*] , L. B. LIMA [1,†] .

[1] Universidade Federal de Mato Grosso do Sul, CPAQ, MS, Brasil,

Submetido em 15/11/2018; Aceito em 13/12/2018; Publicado em 06/09/2019

Resumo. A teoria de design combinatório é uma estrutura que possui importantes padrões relacionados à construções de conjuntos finitos. Essa estrutura combinatória teve suas origens mais formais com os trabalhos de Euler sobre quadrados latinos no fim do século XVIII. Como é uma área recente, os designs combinatórios contêm diversos problemas em aberto. Os designs combinatórios têm aplicações na elaboração e análise de estatística, também dispõem de muitas outras aplicações, como na programação, biologia, matemática, design e análise de algoritmos, redes, teoria de grupos, códigos e criptografia. Além disso, faz uso de conceitos como a de álgebra linear, grupos, anéis, corpo e teoria dos números. Iremos apresentar alguns exemplos de códigos corretores de erros, derivado de modelos simples, do ponto de vista combinatório e de visualização, o plano projetivo $BIBD-(7,3,1)$ e o espaço cubo $3-design(8,4,1)$. Esses códigos são casos especiais de uma família de códigos, chamados códigos de Reed-Muller.

Palavras-chave. Designs Combinatórios, Códigos Corretores de Erros, Geometria de Galois.

Abstract. Combinatorial design theory is a structure that contains important methods related to finite set constructions. This combinatorial structure has its more formal origins with Euler's works on Latin squares the end of the 18th century. As is a recent area, combinatorial designs contain several open problems. Combinatorial designs have applications in the elaboration and statistical analysis, they also have many other applications such as in programming, biology, mathematics, design, and analysis of algorithms, networks, group theory, codes, and cryptography. In addition, it makes use of the concepts of linear algebra, groups, rings, field and number theory. We will present some examples of brokers errors codes, combinatorial point of view and preview, the projective plane $BIBD-(7,3,1)$ and the cube space $3-design(8,4,1)$. These codes are special cases of a family of codes, called Reed-Muller codes.

*jessicarobertaoliveira@yahoo.com.br
†leandro.lima@ufms.br

1 Introdução

A teoria de design combinatório nos traz questionamento de como organizar elementos de um conjunto finito em subconjuntos para que "x" propriedades sejam satisfeitas. Essa estrutura combinatória que teve suas origens mais formais com os trabalhos de Euler sobre quadrados latinos no fim do século XVIII.

A teoria do design surgiu como uma área em Matemática recreativa, mas evoluiu no século XX em uma disciplina de pleno direito matemático com diversas aplicações em estatística e informática. Isso a torna uma das áreas bela da matemática.

Segundo [1], os problemas fundamentais na teoria do design são simples o suficiente para que eles possam ser explicados aos não-matemáticos, no entanto, as soluções dessas questões envolveram o desenvolvimento inovador de novas técnicas combinatórias, bem como engenhosas aplicações de métodos de outras áreas da matemática, como álgebra e teoria dos números.

Os designs combinatórios possuem aplicações na elaboração e análise de estatística, na programação, biologia matemática, análise de algoritmos, redes, teoria de grupos, códigos e criptografia. Também possuem fortes conexões com conceitos de álgebra linear, grupos, anéis, corpo e teoria dos números. Para mais detalhes, veja, por exemplo, [2, 3, 4]. Como é uma área recente (há pouca literatura em português), existem muitos problemas em aberto, o que torna a área muito atrativa. Esta pesquisa se fundamentou principalmente nos textos [5] e [1].

Nesse trabalho exploramos os designs combinatórios, sua estrutura combinatória, suas diferentes formas de representação e construção, onde evidenciamos e utilizamos a relação com a geometria de Galois, para tratar alguns problemas, por meio de exemplos e aplicações de designs combinatórios em teoria de códigos corretores de erros.

2 Metodologia

Inicialmente foram explorados os fundamentos da teoria de design combinatório a fim de explorar as aplicações em plano projetivo e na teoria de códigos corretores de erros. Serão apresentados alguns conceitos da teoria de design encontrados (Veja, por exemplo, [1] e [6], os teoremas e exemplos citados nessa seção podem ser encontrados nessas referências), evidenciando que a mesma é uma importante estrutura de alto grau de regularidade que está relacionada à construção de conjuntos finitos.

Definição 2.1. *Seja $x \neq \emptyset$ um conjunto com v elementos e $B \neq \emptyset$ uma coleção de b subconjuntos distintos de X com cardinalidade $k > 0$. Definimos o par (X, B) por t-design com parâmetros (v, k, λ), onde $0 < t < k < v$ e $\lambda > 0$, se cada subconjunto de cardinalidade t está contido em exatamente λ elementos de B. Usualmente os elementos de B são chamados blocos.*

Consideramos agora os seguintes exemplos:

Exemplo 2.1. *Dizemos que o par (X, B) com $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ e com o*

conjunto de blocos

$B = \{1256, 3478, 1357, 2648, 1458, 2367, 1234, 5678, 1278, 3456, 1368, 2457, 1467, 2358\}$

é um $3-$*design com parâmetros* $(8, 4, 1)$ *(representado na Figura* (1)*), onde* $v = 8$ *(cardinalidade do conjunto* X*), cada 4 (quatro) elementos de* X *estão organizados em cada bloco de* B*, ou seja,* $k = 4$ *tal que cada subconjunto de três elementos* $(t = 3)$ *está contido em apenas um* $(\lambda = 1)$ *bloco do conjunto* B*.*

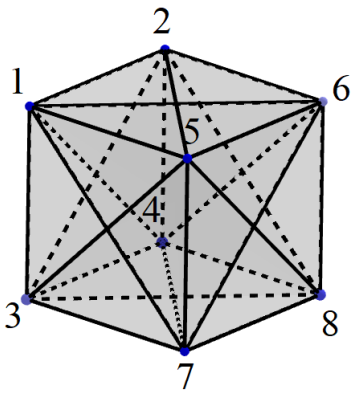

Figura 1: Geometria do 3-design (8,4,1). Fonte: [5]

Exemplo 2.2. *Sejam* $X = \{1, 2, 3, 4\}$ *e* $B = \{123, 234, 134, 124\}$*. O par* (X, B) *é um* $2-$*design com parâmetros* $(4, 3, 2)$ *(representado na Figura* (2)*), onde* $v = 4$ *(cardinalidade do conjunto* X*),* $k = 3$ *tal que cada subconjunto de 3 (três) elementos está organizado em cada bloco de* B*, tal que cada subconjunto de dois elementos de* X *está contido em apenas dois blocos* $(\lambda = 2)$*.*

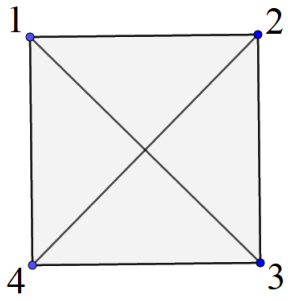

Figura 2: Geometria do 2-design (4,3,2). Fonte: [6]

A classe mais estudada do design é do tipo $t = 2$, em especial os BIBDs (*Balanced Incomplete Block Design*). Demos atenção nesses conceitos, pois essa classe de design encontramos inúmeros aplicação, inclusive com a geometria de Galois.

Definição 2.2. *Seja $x \neq \emptyset$ um conjunto com v elementos e $B \neq \emptyset$ uma coleção de b subconjuntos distintos de X com cardinalidade $k > 0$. Definimos o par (X, B) por $t-$design com parâmetros (v, k, λ), onde $0 < t < k < v$ e $\lambda > 0$, e escrevemos (v, k, λ)-BIBD, se:*

i) Cada bloco de B contém exatamente k elementos;

ii) Cada par de elementos distintos está contido em exatamente λ blocos.

Exemplo 2.3. *O par (X, A) é um $(9, 3, 1)$-BIBD. Com $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e*

$$A = \{123, 456, 789, 147, 258, 369, 159, 267, 348, 168, 249, 357\}.$$

Cada bloco de A possui exatamente 3 elementos de X e quaisquer dois elementos de X estão contidos somente em único bloco.

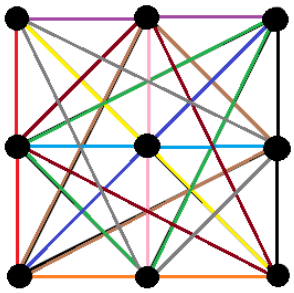

Figura 3: Geometria do (9,3,1)- BIBD. Fonte: [1]

Na Figura (3), temos cada ponto representando os elementos de X, e cada ligação de três pontos representa um bloco de A. Apresentamos também o teorema a seguir, o que nos garante a unicidade do parâmetro de cada BIBD.

Teorema 2.1. *Se (X, B) é um (v, k, λ)-BIBD, então cada elemento de X pertence a r blocos, onde:*

$$bk = rv \text{ e } r(k-1) = \lambda(v-1).$$

Note que não existem (v, k, λ)-BIBD com os parâmetros (8, 4, 2). Pelo teorema anterior, dado que v = 8, k = 4 e λ = 2 temos: r(4-1) = 2(8-1) logo 3r = 14 com isso r = $\frac{14}{3} \notin \mathbb{Z}$ Existe inúmeros outros tipos de design, porém focamos nesses apresentados, onde evidenciamos sua estrutura combinatória, suas diferentes formas de representação e construção.

3 Resultados e Discussões

Dados os fundamentos da teoria de design combinatório na seção anterior, agora podemos entender as aplicações em códigos corretores de erros. Para isso, é necessário uma leitura introdutória sobre a teoria de códigos para entender a aplicação do design em código. Existem inúmeras referências como, por exemplo, [7, 8, 9].

Ao transmitir uma mensagem podem ocorrer ruídos no qual chamamos de erros. A questão é como fazemos para encontrar e recuperar esses erros. A resposta desse questionamento são objetivos dos códigos corretor de erros. A solução mais simples é enviar a mensagens duas vezes, assim verificando cada bits que chega nas duas mensagens. Chamamos de códigos de repetição. Se notarmos um erro (se na duas mensagem algum bit não for igual) não sabemos qual das duas mensagens estão corretas, por isso não podemos corrigi-lo. É um código que detecta um erro, mas não corrige.

Outra maneira de detectar o erro, chamado de verificação de paridade, no qual adicionamos um bit de um dado comprimento, se tivermos uma quantidade par de 1's, adicionamos 0, caso contrário, adicionamos 1. Como o código acima, ele detecta um erro, mas não sabemos em qual posição está o erro. Se errar dois bits, o código não detecta, pois ele continuaria tendo uma quantidade par de 1's.

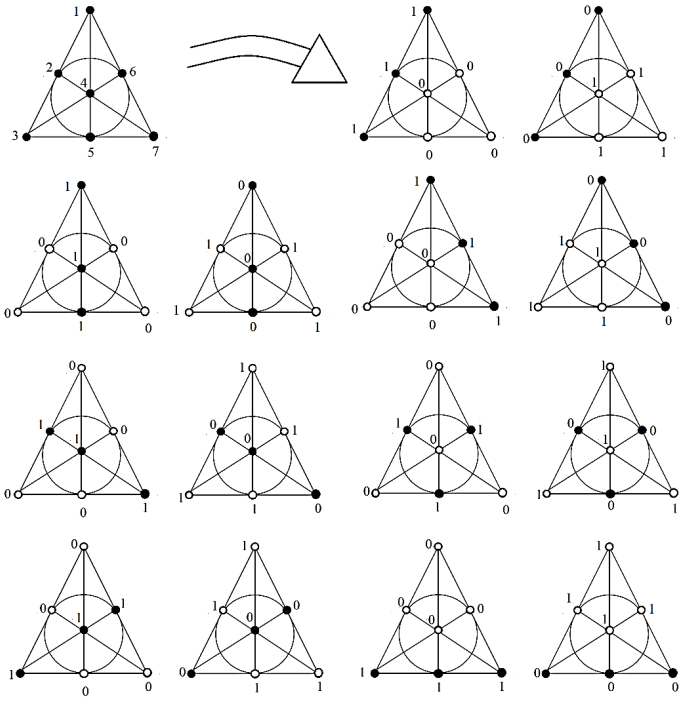

Figura 4: Todas palavras código (7,3,1). Fonte: [2]

Podemos construir um código mais interessante a partir da geometria de Galois. Mostraremos a elaboração no plano de Fano [10] (plano projetivo de ordem 2) e do espaço cubo, onde possuem relação com os designs combinatórios $(7, 3, 1)$-BIBD e $3-design(8, 4, 1)$ respectivamente. Construímos o código a partir dos blocos desses designs.

Com o $(7, 3, 1)$–BIBD, consideramos o par (X, B), onde $X = \{1, 2, 3, 4, 5, 6, 7\}$ e $B = \{123, 145, 167, 247, 256, 346, 357\}$. Em cada bloco, geramos duas palavras-código de cardinalidade 7. Primeiro, adicionamos 1 se pertence ao bloco e 0 se não. Segundo, adicionamos 0 se pertence e 1 se não. Por fim, geramos 14 palavras-código (Figura (4)). Acrescentamos tudo zero (000000) e tudo um (1111111), para obter no total 16 palavras-código.

Com $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ e

$$B = \{1256, 3478, 1357, 2648, 1458, 2367, 1234, 5678, 1278, 3456, 1368, 2457, 1467, 2358\},$$

o par (X, B) é $3 - design$ com parâmetros $(8, 4, 1)$ como visto anteriormente. Representamos esse design através do espaço cubo.

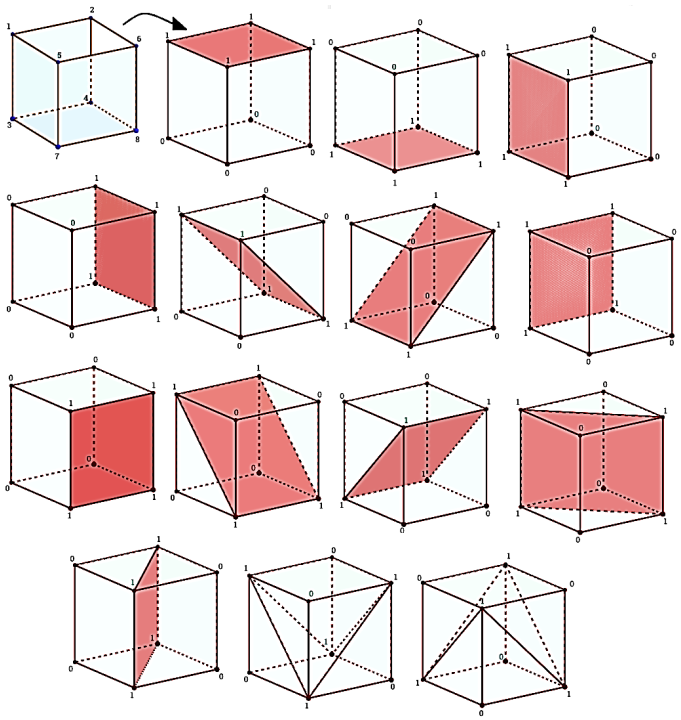

Figura 5: Todas palavras código 3- design (8,4,1). Fonte: [2]

O código gerado por esse design, diferente do anterior ao fixar um bloco gera somente uma palavra-código. Essa palavra-código possui cardinalidade 8, com o

bloco fixado, quando pertence ao bloco adicionamos 1 e 0 se não. No fim são geradas 14 palavras-código (Figura (5)), então, também acrescentamos tudo zero (000000) e tudo um (1111111), para obter no total 16 palavras-código.

Esses códigos não apenas detectam um erro, como também o corrige. Ambos possuem cadeia de 16 códigos, porém o de plano de Fano detecta somente dois erros, pois ao errar 3 bits resulta em outra palavra código. Já o espaço cubo pode detectar 3 erros, mesmo ocorre ao obter 4 erros.

Diante disso, do ponto de vista combinatório e de visualização apresentados, o plano projetivo BIBD-$(7, 3, 1)$ e o $3 - design(8, 4, 2)$ do espaço cubo, são casos especiais de uma família de códigos, chamados códigos de Reed-Müller ([11, 12]). Segundo [2], esses tipos de códigos são importantes na prática, foram usados nas cápsulas NASA Mariner para enviar de volta imagens de Marte, e era baseado em subespaço 3-dimensional de um espaço 5-dimensional, diferente do código do espaço cubo , no qual se baseia em subespaço 2-dimensional de um espaço 3-dimensional.

4 Considerações Finais

A abordagem desse trabalho foi voltada para a teoria de design e a análise da aplicação com a teoria de códigos, sobre a qual foram expostos vários exemplos, a fim de evidenciar sua estrutura combinatória, suas diferentes formas de representação e construção.

Por se tratar de uma área recente, há muito por descrobrir. O intuito desse trabalho é o de elucidar novas pesquisas nessa área, tanto com relação à aplicação em teoria de códigos como aplicações em outras áreas.

Referências

[1] D. STINSON, *Combinatorial Designs: constructions and analysis*. Springer, 2007.

[2] L. LOVÁSZ, J. PELIKÁN, and K. VESZTERGOMBI, *Matemática Discreta*. Textos Universitários, SBM, 2. ed. ed., 2013.

[3] C. J. COLBOURN, *CRC Handbook of Combinatorial Designs*. CRC Press, 2010.

[4] E. S. LANDER, *Topics in Algebraic Coding Theory*. Cambridge University Press, 1983.

[5] C. J. COLBOURN and J. H. DINITZ, *Handbook of Combinatorial Designs*. CRC Press, 2006.

[6] L. B. LIMA, *Contribuições em codificação no espaço projetivo e proposta de códigos quânticos de subespaços na Grassmanniana*. Tese de Doutorado em Engenharia Elétrica, Unicamp, Campinas, Brasil, 2017.

[7] V. PLESS, *Introduction to the Theory of error-correcting codes*, vol. 48. John Wiley & Sons, 1998.

[8] D. J. BAYLIS, *Error Correcting Codes: A Mathematical Introduction*. Routledge, 2018.

[9] R. W. HAMMING, *Coding and Theory*. Prentice-Hall Englewood Cliffs, 1980.

[10] J. HIRSCHFELD, *Projective Geometries over Finite Fields*. Oxford University Press, 1998.

[11] I. REED, "A class of multiple-error-correcting codes and the decoding scheme," *Transactions of the I.R.E. Professional Group on Information Theory*, vol. 4, no. 4, pp. 38–49, 1954.

[12] D. E. MULLER, "Application of boolean algebra to switching circuit design an to error detection," *Transactions of the I.R.E. Professional Group on Electronic Computers*, vol. 3, no. 3, pp. 6–12, 1954.